EXHIBIT D

CENTIMARK
Innovative Roofing and Flooring Solutions

CENTIMARK DEPARTMENTAL POLICY

COMPUTER SYSTEMS

EFFECTIVE DATE: May 1, 1997

POLICY NUMBER: POL-A/G102

REVISION DATE: May 25, 2016

APPROVED BY: _____
Timothy M. Dunlap
President and COO

PURPOSE:
CentiMark has established this policy to govern the use of the CentiMark Computer System to maintain its integrity and lawful orderly use. The Computer System has been developed to facilitate the storage and processing of information and employee communications throughout the corporation.

POLICY:
The CentiMark Computer System must be used in accordance with the standards established herein.

APPLICABILITY:
This policy applies to all employees of CentiMark Corporation.

DEFINITIONS:

CentiMark Computer System:
All hardware and all software, whether owned and/or leased by the company, and including any and all information contained therein, and specifically including e-mail and all messages or images created therein.

Authorized Company Personnel:
A team consisting of an employee's supervisor or department manager and a management representative of management information services.

Approved Software:
Software that has been reviewed and approved in writing for use by CentiMark authorized personnel, which shall include certifying the software free of any virus.

DISCUSSION/POLICY MECHANICS:

1. The CentiMark computer system in all its parts, whether owned or leased, is the exclusive business property of CentiMark Corporation and should be used for business purposes only.

2. Information in possession of current or former CentiMark employees, regardless of its origin, that relates to CentiMark, its suppliers, customers, employees or any other entity related to CentiMark shall be considered the sole property of CentiMark. This policy is in force regardless of the ownership status of the computer system that contains that information.

3. No employee has a right of privacy in any file or information created, used or stored on the CentiMark computer system, including the e-mail system, regardless of whether the employee considers such files to be personal. Use of or information contained within any part of the CentiMark Computer System, including access to the Internet and the e-mail system may be monitored and/or subject to audit.

4. Each employee with a CentiMark e-mail account is expected to routinely access their e-mail to review, respond and process new e-mail messages in a timely manner. All e-mails whether received or created by the account holder are the property of CentiMark. CentiMark recognizes that the ability to transmit messages electronically is an essential part of business communications. Similar to other types of documents, CentiMark has established a retention period that balances the need to manage and view historical messages with the cost and risk of perpetual storage. As a result, e-mails exceeding three years from the date of creation will be automatically deleted on a daily on-going basis.

5. CentiMark does not condone the use of the CentiMark computer system in such a way that its illegal, regardless of whether or not the employee knew the use was illegal, including but not limited to:

   Installing, copying, uploading or downloading, or using any unauthorized software is a violation of this policy. Approved software is software that has been approved for use by CentiMark authorized personnel.

   Creating, passing, or saving any message, file or other communication, the content of which could be considered offensive, demeaning, or disruptive to any person, or which could be construed to create a hostile or abusive work place environment which would offend someone based on their race, color, sex, religion, national origin, age, physical or mental disability, or status as a veteran is a violation of company policy.

6. All information used or created on the CentiMark computer system is subject to inspection by authorized company personnel and review at any time without any prior notice.

7. CentiMark will delete from the Computer system any unauthorized software found on the company owned computer system.

8. Monitoring of the CentiMark Computer System will be performed in a non-discriminatory manner under the direction of a member of Management who is trained in avoiding discriminatory actions and Management of the Information System department.

9. It is the responsibility of every employee to safeguard the company, including its business, proprietary and confidential information. Therefore, no employee may copy, download, or in any other manner appropriate (whether in whole or in part) any of the data base(s), files, information, programming or software contained on any part of the CentiMark computer system for use in any manner not specifically related to the performance of employment duties for CentiMark. No employee may use or distribute software, information, file or database that is a violation of the license agreement for the hardware or software.

10. CentiMark must take every precaution to protect the computer system from contamination by viruses. Therefore, no employee may upload, download, appropriate from or add to the CentiMark computer system from any external source, including from a home computer, without prior approval from authorized company personnel.

11. It is the responsibility of every employee to take reasonable precautions to safeguard CentiMark computer, communications, imaging and other related equipment. In cases of lost, stolen or damaged equipment management will determine on a case by case basis if either negligence or misconduct caused the loss. If negligence or misconduct contributed or caused the loss, the employee may be responsible for a minimum of 50% of the original purchase price, but not more than the current fair market value, determined by Information Systems management, at the time of loss. If damaged equipment can be repaired, and management chooses to have the equipment repaired, the employee will be liable for a minimum of 50% of the cost of the repair. An example of negligence would be to leave computer equipment anywhere in the passenger area of the car. Computer equipment should be locked in the trunk. If the vehicle has no trunk, equipment should be removed or concealed in a hidden compartment if available, 'behind the front seat' is not a hidden compartment. Equipment that is lost, misplaced, or stolen from any type of public setting like an airport or hotel lobby is considered negligence for failing to properly secure the equipment. Conversely, if equipment is in a car that is stolen or a hotel room that is burglarized, and the employee took reasonable precautions to secure the equipment, then the determination would be there was no negligence. Misconduct is any type of deliberate act that damages the computer equipment.

12. Every employee has an affirmative duty to return any and all files and/or information in his or her possession at the time of the termination of employment, regardless of whether the employee had permission to have the information in his or her possession.

13. Violations of the policy are to be reported to an employee's department manager, the human resources department or the legal department. A request for anonymity in

reporting any violation will be respected to the fullest extent possible, and no employee shall be subject to retribution for complying with this policy. Violation of this policy by an employee may result in disciplinary action up to and including termination of employment.

Passwords

Passwords are an important aspect of computer security. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Passwords are used for various purposes at CentiMark. Some of the more common uses include: network access, e-mail, various business applications including SAP, screen saver protection, and voicemail passwords. Many applications utilize one common password, so it is vital that all users understand how to develop strong passwords.

CentiMark Minimum Password Standards:

- A password of eight (8) characters or more and
- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Any three (3) of the four (4) items below:
    - one Upper Case letter (A through Z)
    - one lower case letter (a through z)
    - one number (1 through 9)
    - one non-alphabetic character (for example; !, @, #, $, %)

You will need to maintain two passwords to access CentiMark's computer systems – One password for Google (Gmail, etc.) and a second password for Windows. CentiMark's Minimum Password Standards apply to both. Additionally, any 3rd party system accessed for business purposes that has a unique User ID and Password should adhere to CentiMark Minimum Password Standards. Password standards are enforced for Microsoft Windows when passwords are changed or created. Google and other 3rd party systems may not allow CentiMark to enforce Minimum Password Standards; however, all employees are responsible for utilizing passwords in accordance with this Company Policy.

Poor, weak passwords have the following characteristics:

- Names or derivatives of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "<Company Name>", "sanjose", "sanfran" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that

can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss or co-workers
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't record passwords on paper kept in the office.

Passwords are NOT to be shared on a routine or non-temporary/non-emergency basis.

DISTRIBUTION OF POLICY:

Upon final approval, this Policy will be distributed to each field office for filing in the CentiMark Policy Manual. A copy is also available on the Centranet.

POLICY/PROCEDURE CROSS REFERENCE:

Not applicable.

COMMUNICATION:

Senior Management and the Executive Committee are responsible for reinforcing the purpose and intent of this document throughout their respective areas.